UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/604,174	06/27/2000	John L. Manferdelli	MSFT-0188/154574	4724

41505 7590 09/13/2007

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)
CIRA CENTRE, 12TH FLOOR
2929 ARCH STREET
PHILADELPHIA, PA 19104-2891

EXAMINER	
BROWN, CHRISTOPHER J	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
09/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/604,174	MANFERDELLI ET AL.	
	Examiner	Art Unit	
	Christopher J. Brown	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 July 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-73* is/are pending in the application.

4a) Of the above claim(s) *22-73* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☒ Claim(s) *1* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

Applicant's election with traverse of a method for creating a computer program that performs actions of a cryptographic program without requiring the cryptographic program's key. in the reply filed on 7/10/2007 is acknowledged. The traversal is on the ground(s) 1) There is no serious burden on the examiner. 2) There is no reason why the groups are characterized as subcombinations that are distinct from each other 3) C.F.R 1.142 states that a restriction requirement should be made before final action. This is not found persuasive because 1) the groups of claims do place a serious burden on the examiner, the fact that the application was not previously restricted does not negate the fact that the application places a serious burden on the examiner because of the differing claim groups. 2) The examiner illustrated that the groups in the restriction were directed towards different classes and purposes. 3) This restriction was made after a non-final action on the merits.

The requirement is still deemed proper and is therefore made FINAL.

Response to Arguments

Applicant's arguments with respect to claim 1 have been considered but are moot in view of the new ground(s) of rejection in view of Aucsmith US 5,892,899

As per applicant's argument that Granger US 6,643,775 requires access to cryptographic key. The examiner asserts that the Granger reference is ambiguous with respect to said

key. Granger teaches writing the encryption engine and key generator in pseudocode or obfuscating said key generator and encryption engine. If the key is incorporated as part of the encryption engine then the encryption engine written in pseudocode, or obfuscated, does not need to access said key. Granger is unclear as to the status of the key, Hence the incorporation of Aucsmith.

Applicant argues that Granger requires access to said cryptographic key, but that the instant invention does not. Examiner admits the computer executable instructions and computer program do not explicitly access the cryptographic key. However, two arguments must me made with regard to claim 1. First, The computer program, in its *creation* does require access to cryptographic key. In that aspect, the computer program does require access to said cryptographic key. Second, the applicant must define when the key ceases to become the key. If the computer program incorporates elements of the key or its actions into instructions, it inherently contains and "accesses" the key, or incorporates the key, even if the key is not in the same data form previously seen. The applicant must further define the invention through the claims in order to further prosecution.

Also the examiner would like to state for the record that the language used in claim 1 makes optional "does not require access to a cryptographic key". MPEP 2106 states that language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation. The following are examples of language that may raise a question as to the limiting effect of the language in a claim:

(A) statements of intended use or field of use,

(B) "adapted to" or "adapted for" clauses,

(C) "wherein" clauses, or

(D) "whereby" clauses.

In the instant case "does not require access said cryptographic key" is not a step.

Examiner encourages the applicant to write the claim as a series of positively receited steps.

Claim Objections

Claim 1 is objected to because of the following informalities: The applicant appears to be missing the "to" in "access **to** said cryptographic key" on the last line of claim 1.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: the steps to transform the computer instructions to perform the actions of the key, where the instructions or program do not access the cryptographic key directly.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 2, 8, 10, 12, and 21 are rejected under 35 U.S.C. 102(b) as being anticipated by Aucsmith US 5,892,899.

As per claim 1, Aucsmith teaches identifying a set of actions that are performed in the course of using a cryptographic algorithm to apply a cryptographic key to said first data (a security sensitive program that uses a secret "S" to implement a cryptographic function) (Col 4 lines 1-15). Aucsmith teaches generating a first set of computer-executable instructions which includes instructions to perform said actions (generates partitioned subparts) (Col 3 lines 48-57). Aucsmith teaches including said first set of computer-executable instructions in said computer program, wherein said computer program does not require access said cryptographic key (subprogram generator for generating subprograms to implement a security sensitive program that does not require access to a secret, secret data is partitioned, thus eliminating secret data) (Col 4 lines 3-5).

As per claim 2, Aucsmith teaches said cryptographic algorithm is a public/private-key algorithm (asymmetric key scheme) (Col 4 lines 10-16).

As per claims 8, 10 Aucsmith teaches generating a diversionary second set of computer-executable instructions which perform one or more second actions; and including said second set of computer-executable instructions in said computer program (tasks to further obscure the true nature of the program, these tasks have no purpose) (Col 4 lines 15-20).

As per claim 12 Aucsmith teaches reorganizing at least some code contained in the program (obfuscated by dividing and processing into a number of obfuscated subprograms) (Col 5 lines 18-22).

As per claim 21 Aucsmith teaches a set of instructions to perform claim 1 (subprogram generator) (Col 4 lines 20-25).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3 and 7, 14-16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith US 5,892,899 in view of Granger US 6,643,775.

As per claim 3 Aucsmith teaches secret and a asymmetric algorithm, but does not teach that the secret is a private key of an asymmetric key pair.

Granger teaches that the secret is a private key of an asymmetric key pair (key in an asymmetric algorithm) (Col 10 lines 28-38).

It would have been obvious to one of ordinary skill in the art to use the asymmetric key of Granger as the secret in Aucsmith because it is beneficial to hide keys from software pirates.

As per claim 7 Aucsmith fails to teach pseudo-randomly generating a number, wherein said first set of computer-executable instructions is based on said number.

Granger teaches pseudo-randomly generating a number, wherein said first set of computer-executable instructions is based on said number (during encryption multiplies by random number R) (Col 12 line 55).

As per claim 14, Aucsmith fails to teach encrypting a portion of instructions.

Granger teaches encrypting at least a portion of said first set of computer-executable instructions; and creating a second set of computer-executable instructions which decrypts said portion (encrypts data table, decrypts line by line when needed) (Col 7 lines 8-20).

As per claim 15, Aucsmith does not specify source level code.

Granger teaches the program is written in source and compiled, (high level language, then compiled) (Col 7 lines 53-59).

As per claim 16, Aucsmith does not teach postprocessing.

Granger teaches the act of postprocessing the compiled instructions after said compiling act, wherein said postprocessing act comprises one or more of the following: encrypting at least a portion of the compiled instructions, and hashing at least a portion of the compiled instructions (encrypting after compiling) (Col 15 lines 18-21).

Claim 4-6, 17, 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith US 5,892,899 in view of Maytal US 6,715,079.

As per claims 4, 5, and 6 Aucsmith teaches a secret as second data but fails to teach the secret in some way identifies or relates to a computing device on which said computer program runs, and wherein said first set of computer-executable instructions is based on said second data.

Maytal teaches using a second data that identifies a computing device on which said computer program runs and wherein said first set of computer executable instructions is based on said second data (uses the CPUID as the secret/second data that is incorporated into computer executable instructions) (Col 10 lines 25-35). It is well known that proper execution depends on retrieval of second data (proper encryption/decryption needs correct operations based on incorporated data).

It would have been obvious to one of ordinary skill in the art to use the CPUID of Maytal with the program of Aucsmith because it will prevent illegal copying and use without the appropriate hardware.

As per claims 17 and 18, Aucsmith does not teach receiving, from a computing device, a request for said computer program via a network; and

providing said computer program to said computer device via said network where the network is the internet.

Maytal teaches receiving, from a computing device, a request for said computer program via a network; and providing said computer program to said computer device via said network where the network is the internet.(CPU's submitting data to request a customized computer program may be downloaded to the computer over the Internet) (Col 10 lines 25-35).

Claims 9,and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith US 5,892,899 in view of Matsui US 2002/0178412.

As per claims 9, and 20 Aucsmith teaches diversionary code (Col 4 lines 15-20).

Aucsmith does not teach retrieving instructions from a database.

Matsui teaches retrieving instructions from a database (retrieving program from external database and compiling it) [047].

It would have been obvious to one obvious to one of ordinary skill in the art to modify Aucsmith with the database of Matsui because it can be retrievable at any terminal with network access.

Claim 11, is rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith US 5,892,899 in view of Barton US 5,912,972

As per claim 11, Aucsmith fails to teach a second set of computer-executable instructions which detects modification or deletion of at least a portion of code contained in said computer program, and which restores said portion if said portion has been deleted or modified.

Barton teaches error detection and correction, (Col 9 lines 9-16).

It would have been obvious to one of ordinary skill in the art to add the error correction to n the system of Aucsmith because the error correction would maintain the data and prevent errors.

Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith US 5,892,899 in view of Mirov 6,138,236.

As per claim 13 Aucsmith teaches generating instructions in a computer program.

Aucsmith does not teach delimiting or hashing.

Mirov teaches delimiting a segment of at least some code contained in a program (micro code) (Fig 1). Mirov teaches obtaining a first hash of the code (verification hash) Mirov teaches obtaining a second hash (data hash) and comparing the first hash with the second hash (comparing data hash with verification hash to determine authenticity)(Fig 4 Col 4 lines 8-26).

It would have been obvious to one of ordinary skill in the art to use the authentication of Mirov with the program of Aucsmith because it prevents the use of code that may have been tampered with.

Claims 19, is rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith US 5,892,899 in view of Maytal US 6,715,079 in view of Frasier US 5,758,293

As per claims 19, Aucsmith does not disclose downloading a program over the Internet. Maytal teaches CPU's submitting data to request a customized computer program may be downloaded to the computer over the Internet, (Col 10 lines 25-35). Maytal does not specify the timetable for downloading.

Frasier teaches that data is downloaded contemporaneously with a request for said data, (Col 1 lines 17-23). It would have been obvious to use the contemporaneous download of Frasier with Maytal because it allows for the quick transfer of data.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher J. Brown 9/8/07